REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed January 4, 2005. In the Office Action, claims 1-2, 6-8, 10, 12, 14, 19-20, and 22 were rejected under 35 U.S.C. §102, and claims 3, 4, 5, 9, 11, 13-14, 15, 16, 17, 18, 21, 23, and 24 were rejected under 35 U.S.C. §103. Herein, claims 1, 8 and 20 have been cancelled without prejudice. Claims 2-7, 9-15, 17 and 21-23 have been revised. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

In the specification, new paragraph [0021] has been added prior to former paragraph [0021]. As a result, original paragraphs [0021] to [0024] have been renumbered as paragraphs [0022] to [0025]. Newly renumbered paragraph [0022] has been amended to correct minor editorial problems.

Specification

The specification was objected to because the provisional application number was not correctly identified due to a typographical error. Applicant respectfully corrects the typographical error and corrects the claim of priority.

Hence, Applicant respectfully requests that the Examiner withdraw the objection to the specification.

Rejection Under 35 U.S.C. § 102

Claims 1-2, 6-8, 10, 12, 14, 19-20, and 22 were rejected under 35 U.S.C. §102(b) as being anticipated by Tatu Ylonen (U.S. Patent No. 6,782,474). Applicant respectfully traverses the rejection in its entirety because a *prima facie* case of anticipation has not been established.

As the Examiner is aware, to anticipate a claim, the reference must teach each and every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Vergegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989).

Herein, Applicant respectfully submits that a *prima facie* case of anticipation has not been established because Tatu Ylonen does not teach each and every element set forth in pending independent claims 1, 8 and 20.

For instance, the Office Action states that the device identifier of Tatu Ylonen is equivalent to the "device identification" and the cryptographic key could be considered as "one key corresponding to the device identification." *See Limitation 1a) of Page 3 of the Office Action.* However, if the device identifier teaches the "device identification," then Tatu Ylonen does not teach the transmission of a message comprising the device identification. However, it

appears that the Examiner has mistakenly deviated from this original analysis when determining whether other limitations are taught by Tatu Ylonen.

As an example, the Office Action states that the 32-bit Security Association identifier is equivalent to the "device identification" in order to support an allegation that Tatu Ylonen teaches transmission of a message comprising the device identification. *See Limitation 1c) of Page 3 of the Office Action.* But, the Examiner now improperly considers two separate items as being equivalent to the device identification. As yet another example, the Office Action states that the shared secret key is equivalent to the device identification. *See Limitation 1d) of Page 4 of the Office Action.* Now, the Examiner considers three separate items as being the device identification.

Such analysis appears to constitute impermissible hindsight reconstruction, and thus, Applicant respectfully requests the Examiner to withdraw the outstanding §102(b) rejection.

Rejections Under 35 U.S.C. § 103

A. CLAIM 3

Claim 3 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell (U.S. Patent No. 4,605,820). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. Applicant has placed claim 3 into independent format, including limitations from original base claim 1.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the cited references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine the teachings of references. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or combination of references) must teach or suggest all of the claim limitations. *See MPEP §2143; See also In re Fine,* 873 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). At a minimum, the combination of the cited references does not teach or suggest all of the claim limitations.

As stated on Page 3 of the Office Action, the device identifier of Tatu Ylonen is deemed to be equivalent to the "device identification" as claimed." *See Limitation 1a) of Page 3 of the Office Action.* However, the device identifier is derived from an appropriate cryptographic key, which directly contradicts the claimed invention where the device identification is used to generate the key. *See lines 3-4 of claim 3.*

Moreover, the claimed invention claims that the at least one key is generated using the device identification and a plurality of generation keys. It is alleged that the combined teachings of Tatu Ylonen and Campbell teaches this limitation. However, Applicant respectfully disagrees because neither Tatu Ylonen nor Campbell, alone or in combination, teach the generation of at least one key(s) for encoding data using the device identification and a plurality of generation keys, especially where the device identification is included in a header of a message including the encoded data.

As an example, it is alleged that a person skilled in the art at the time of the invention would have implemented the key management system of Campbell into the network connectiable device of Tatu Ylonen. In other words, it is alleged that the claimed invention is unpatentable because the combined teachings of Tatu Ylonen and Campbell, which teaches the generation of the fifty (50) values (considered "generation keys") forming the primary key table based on the initial double-length key (considered "device identification"). *See Page 10 of the Office Action.* Applicant disagrees for a number of reasons, some of which are enumerated below.

First, it is noted that the initial double-length key of Campbell is generated by a security module and appears to remain resident in the device featuring the PIN pad for security reasons. Second, Campbell is devoid of any teaching or suggestion of generating "the at least one key," considered to be the cryptographic key of Tatu Ylonen, based on the initial double-length key (*device identification*) and a *plurality of* generation keys. *Emphasis added.* Rather, Campbell teaches generation of a first series of generation keys using the initial double-length key, and subsequent series of generation keys are produced using a selected generation key without using the initial double-length key. There is no collective key usage of the initial double-length key and a plurality of generation keys to produce a resultant key as claimed.

In light of the foregoing, Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claim 3.

B. CLAIM 4

Claim 4 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

Applicant agrees that Tatu Ylonen fails to disclose "further comprising generating the at least one key using a multistage process...." *See Page 12 of the Office Action.* However, Campbell does not disclose this limitation because the key management system of Campbell is directed to the formulation of a table of generation keys using an alleged multistage process, but it does not teach or even suggest a multistage process for the generation of the at least one key as claimed.

In light of the foregoing, Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claim 4.

C. CLAIM 5

Claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell. Applicant respectfully traverses the rejection and respectfully requests the Examiner to reconsider the allowability of the claim as amended and withdraw the outstanding §103(a) rejection.

D. CLAIM 9

Claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell and Marino (U.S. Patent No. 6,026,165). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. However, further discussion as to allowability is moot based on its dependency on claim 11.

Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claim 9.

E. CLAIM 11

Claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell. Applicant agrees that Tatu Ylonen fails to disclose "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." *See Page 16 of the Office Action.*

More specifically, the claimed invention claims that "the at least one key" is generated using the *device identification* and the generation *keys*. *Emphasis added.* However, neither Tatu Ylonen nor Campbell, alone or in combination, teach or suggest the generation of the at least one key, claimed for use in encoding data, based on both the device identification and the generation keys. In fact, the cryptographic key of Tatu Ylonen, alleged to be equivalent to "the at least one key," is used to produce the device identifier, and thus, teaches away from the claimed invention. Even if the initial double-length key of Campbell may be construed as the "device identification" and the 50 values are construed as the "generation keys," both the initial double-length key and the values are not used to generate a resultant key. Rather, the initial double-length key is used to generate a first series of "generation keys" and a selected generation key is used to generate subsequent generation keys. Rather, there use is mutually exclusive, not collective as claimed.

In light of the foregoing, Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claim 11.

F. CLAIMS 13-15 AND 21

Claims 13-15 and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Marino. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. However, further discussion as to allowability is moot based on its dependency on claim 11 or claim 23.

Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claims 13-15 and 21.

G. CLAIM 23

Claim 23 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell. Applicant agrees that Tatu Ylonen fails to disclose "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." *See Page 28 of the Office Action.*

As previously stated, neither Tatu Ylonen nor Campbell, alone or in combination, teach or suggest the generation of the at least one key, which is used for encoding data, based on both the device identification and the generation keys. In fact, the cryptographic key of Tatu Ylonen, which is allegedly equivalent to "the at least one key," is used to produce the device identifier, not the other way around. Even if the initial double-length key is construed as the "device identification" and the 50 values are construed as the "generation keys," both the initial double-length key and the values are not used to generate a resultant key. Rather, the initial double-length key is used to generate a first column (series) of keys and a selected key from that series is used to generate subsequent generation keys. The use of these parameters is mutually exclusive, not collective as claimed.

In light of the foregoing, Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claim 23.

H. CLAIMS 16-18, 24

Claims 16-18 and 24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tatu Ylonen in view of Campbell. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. However, further discussion as to allowability is moot based on theirdependency on claim 11 or claim 23.

Applicant respectfully requests the Examiner to withdraw the outstanding §103(a) rejection as applied to claims 16-18 and 24.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 05/04/2005

By _____
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: 05/04/2005

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

Susan McFarlane 05/04/2005
Susan McFarlane *Date*